

一种二维混沌加密彩色图像自适应水印算法

黄春杨, 龚 劬, 黄秋柳

(重庆大学 数统学院, 重庆 400044)

摘 要:数字水印技术可以有效地保护数字产品的版权,维护数据安全。现有的数字水印方法大多数针对灰度图像,而较少研究彩色图像。但是与灰度图像水印相比,彩色图像水印含有更多的信息。因此,文中提出了一种二维混沌加密的彩色图像自适应水印算法。经过二维 logistic 混沌迭代生成加密水印。在水印嵌入过程中,把彩色图像亮度分量分成互不重叠的图像块,用分数盒维数分析各块的特征,提取特征块和次特征块,对它们分别进行一级小波分解,先将水印以不同强度自适应地嵌入到特征块的小波域低频子图中,在保证隐蔽性的前提下,再次将水印以不同强度自适应地嵌入到次特征块的小波域低频子图中。实验结果表明,该算法对 JPEG 压缩、加噪、剪切、滤波等具有较强的稳健性。

关键词:数字水印; 分数盒维数; 二维 logistic 混沌; 彩色图像

中图分类号: TP309

文献标识码: A

文章编号: 1673-629X(2010)02-0141-04

Color Image Watermarking Algorithm Based on Two Dimension Chaotic Encryption

HUANG Chun-yang, GONG Qu, HUANG Qiu-liu

(College of Mathematics and Physics, Chongqing University, Chongqing 400044, China)

Abstract: Digital watermark technique is effective in protecting copyright of digital products and maintaining data security. Existing digital watermarking algorithms are mostly designed against gray images but few are for the color images. This paper presents a color image watermarking algorithm based on two dimension chaos encryption. Use the two dimension logistic chaotic map to generate the watermark. An original image is divided into non-overlapped blocks, fractional box-counting dimension is used to analyze the feature of the image blocks to extract the feature blocks and secondary feature blocks and then used one level DWT to decompose them. The different strength watermark is adaptively embedded into the low-frequency coefficients of the feature blocks, under the condition that the watermark embedded is invisible, and then is embedded into the secondary feature blocks in the same way when embedded watermarking. Experimental results demonstrate that the watermarking scheme is strongly robust to different types of attacks such as JPEG compression, noise addition, cropping, filtering and so on.

Key words: digital watermarking; fractional box-counting dimension; two dimension chaotic; colour image

0 引言

近几年,数字水印技术在版权保护方面的研究十分广泛。混沌序列相对于普通的伪随机序列具有显著的优点,其安全性强,易生成其低通特性,因而可以抵抗低通滤波或 JPEG 压缩攻击等^[1,2],但近年来的研究表明,低维混沌序列的保密性是不够的^[3]。文中算法采用二维混沌系统生成的混沌,对水印序列做预处理以提高水印的安全性。同时嵌入算法充分利用图像自身的特征,用分数盒维数分析宿主图像块的特征,提

取特征块和次特征块,将置乱后的水印以不同强度自适应地嵌入到特征块的小波域低频子图中,在保证隐蔽性的前提下,再次将置乱后的水印以不同强度嵌入到次特征块的小波域低频子图中。

实验证明文中算法对 JPEG 压缩、加噪、剪切等具有较强的稳健性,很好地解决了保真度和嵌入水印强度等问题。

1 二维 Logistic 混沌映射系统

混沌信号对初始条件的极端敏感性,初始条件微小差异,随着迭代次数的增大,将以指数速度分离,变得互不相关^[4]。此外,它还具有各态历经性、非周期、宽频谱性,因而用这种方法加密的信息很难破译,具有很高的保密度。文献[5]介绍了参数化二维混沌映射

收稿日期:2009-06-08;修回日期:2009-09-03

作者简介:黄春杨(1984-),女,硕士研究生,研究方向为小波分析与图像处理;龚 劬,教授,博士,研究方向为图像处理、小波分析、图论与组合优化、逼近理论及其应用、数学建模。

在空间域对图像进行加密的算法,文献[6]介绍了利用 Arnold 变换和 Fibonacci-Q 变换对数字图像进行加密的算法。文献[7]介绍一种二维 Logistic 混沌序列矩阵的生成方法,用其生成加密模板和治乱序列,讨论用其对图像的离散小波变换系数矩阵进行调整和置乱处理问题。

仿真结果表明该混沌序列加解密算法扩展了密钥空间,密文均匀分布,能够克服低维混沌动力学系统易于攻击的缺陷,抵抗选择明文攻击,具有密图文件保密性高,密钥简单,重构图像与原图像一致性良好等特点,并且能够经受住传输过程中噪声的影响。

二维 Logistic 映射混沌点集不存在有效的无误差构造形式^[8],比一维 Logistic 映射有更安全的加密效果。因此,文中研究用二维 Logistic 映射生成混沌序列。

1.1 二维 Logistic 映射定义

根据一维 Logistic 映射^[9],定义二维 Logistic 映射为

$$\begin{cases} x_{n+1} = 4\mu x_n(1-x_n) + g_1(x_n, y_n) \\ y_{n+1} = 4\mu y_n(1-y_n) + g_2(x_n, y_n) \end{cases} \quad (1)$$

其中 g_1 和 g_2 是耦合项,可取两种情况:即 $g_1 = v y_n$ 和 $g_2 = u x_n$ 的一次耦合项,或 $g_1 = g_2 = u x_n y_n$ 的对称一次耦合项。采用具有对称一次耦合项形式的二维 Logistic 映射为

$$\begin{cases} x_{n+1} = 4\mu x_n(1-x_n) + v y_n x_n \\ y_{n+1} = 4\mu y_n(1-y_n) + u x_n y_n \end{cases} \quad (2)$$

式中动力学行为由控制参数 μ_1, μ_2 和 v 决定。

1.2 置乱序列的生成

选择控制参数为 $\mu_1 = \mu_2 = \mu = 0.9, v = 0.13$, 初始点为 $(x_0, y_0) = (0.10, 0.20)$, 用具有对称一次耦合项的二维 Logistic 混沌映射序列迭代,得到两组矩阵 X, Y 。矩阵 X, Y 中的元素一一对应。若待置乱矩阵的大小为 $m \times n$ (其中 m 为矩阵的行数, n 为矩阵的列数), 生成混沌序列 X, Y 的长度为 $p_0 + \frac{m \times n}{8}$ 。因为如果初始点特别相近,混沌序列的前几十个点可能相同,故舍去前 p_0 对值(文中取 $p_0 = 274$), 后 $\frac{m \times n}{8}$ 对值生成置乱序列。将 $X(p), Y(p)$, 其中 $p = 1, 2, \dots, \frac{m \times n}{8}$, 分别乘以 15, 用 round 函数转化为 0 到 15 的整数。再转化为二进制数,使得 X, Y 为 $(\frac{m \times n}{8}) \times 4$ 的新矩阵。新矩阵 X, Y (X 占据矩阵 K 的前四列, Y 占据矩阵的后四列) 组成 $(\frac{m \times n}{8}) \times 8$ 的置乱矩阵 K 。将矩阵 K 用 reshape 函数变形为 $m \times n$ 的矩阵 K' 。

2 水印的嵌入与提取算法

2.1 水印的嵌入

为了抵抗剪切、替换等攻击,水印在嵌入前需要运用置乱技术进行预处理^[10]。通过置乱将水印图像像素的空间位置进行重新排列,以此来消除像素的空间相关性,在载体图像被部分破坏时可以分散错误比特的分布,从而提高了水印的鲁棒性。由分形编码理论知,分形维数可以用来刻画图像表面的纹理信息。一般图像块的分形维数越大,那么它包含的纹理信息就越多;反之,则越平滑。分形维数的类型很多,例如 Hausdorff 维数、关联维、信息维、盒维数等^[11]。J. Feng 在其博士论文^[12]中,在普通盒维数的基础上提出了分数盒维数。对分形维数提供了更精确的计算方法。文中采用分数盒维数分析宿主图像块的特征,提取特征块和次特征块,将置乱后的水印以不同强度自适应地嵌入到特征块的小波域低频子图中,进一步增强了水印的稳健性。根据各块的分数盒维数的大小,使水印自适应地嵌入到彩色图像的亮度分量中。

算法的具体步骤如下:

步骤 1 水印的预处理:水印像素为 $m \times n$, 用密钥 key1 将系数矩阵 L_1 进行六次 Arnold 变换,打乱其像素的空间相关性,从而生成水印图像 L_2 。将 L_2 与置乱矩阵 K' 进行异或运算,得到水印图像 L' 。

步骤 2 利用

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.3316 & -0.50 \\ 0.50 & -0.4186 & -0.0813 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad (3)$$

将原始图像 I 转换到 YCbCr 彩色空间,提取其亮度分量 $Y^{[13]}$ 。

步骤 3 对 L' 进行 2×2 分块,升序排列为 $L'_i, i = 1, 2, \dots, \frac{m}{2} \times \frac{n}{2}$

步骤 4 对 Y 进行 4×4 分块,升序排列为 $Y_i, i = 1, 2, \dots, \frac{M}{2} \times \frac{N}{2}$

步骤 5 分别计算 Y_i 的分数盒维数,降序排列为 $Y'_i, i = 1, 2, \dots, \frac{M}{2} \times \frac{N}{2}$ 。用密钥 key2 产生一组长度为 $\frac{m}{2} \times \frac{n}{2}$, 区间为 $(0.9, 1)$ 的随机数。再将这组随机数按降序排列,前 $\frac{m}{4} \times \frac{n}{2}$ 个有序数记为: $R_1(p), p = 1, 2, \dots, \frac{m}{4} \times \frac{n}{2}$ 。后 $\frac{m}{4} \times \frac{n}{2}$ 个有序数记为 $R_2(p), p = \frac{m}{4} \times \frac{n}{2} + 1, \dots, \frac{m}{2} \times \frac{n}{2}$ 。

对所有 Y_i 进行一级小波分解,得到低频子带 LL'_i , 将水印块按如下公式依次嵌入到 LL'_i 中。

$$LL'_i =$$

$$\begin{cases} LL'_i + [R_1(p) \times Y'_i]^{a_1} \times L'_i, p = 1, 2, \dots, \frac{m}{4} \times \frac{n}{2} \\ LL'_i + [R_2(p) \times Y'_i]^{a_1} \times L'_i, p = \frac{m}{4} \times \frac{n}{2} + 1, \dots, \frac{m}{2} \times \frac{n}{2} \end{cases} \quad (4)$$

用 LL'_i 代替 LL_i , 进行反小波变换得到图像块 Y_i , 再用 \hat{Y}_i 代替 Y_i 。

步骤6 按维数大小依次取出从第 $\frac{m}{2} \times \frac{n}{2} + 1$ 个到第 $\frac{m}{2} \times \frac{n}{2} \times 2$ 个的分数盒维数对应的图像块 Y'_i , 用密钥 key_3 产生一组长度为 $\frac{m}{2} \times \frac{n}{2}$ 的区间 $(0.9, 1.0)$ 上的随机数, 将 a_1, a_2 分别改为 a_3, a_4 。按照步骤5中在图像块 Y_i 中嵌入水印的方法, 再一次将水印信息嵌入到图像块 Y'_i 中。得到含水印的亮度分量 Y' 。

步骤7 用嵌入水印的亮度分量 Y' 代替原来的亮度分量 Y , 并将图像由 YCbCr 彩色空间转化到 RGB 彩色空间, 从而得到嵌入水印的载体图像 I' 。

2.2 提取算法

水印的提取基本上是逆过程:

分别对待检测图像 I' 和宿主图像 I 转换到 YCbCr 彩色空间, 提取其亮度分量 Y' 和 Y , 按照嵌入算法中对宿主图像分块, 对宿主图像经过嵌入算法的步骤5后, 按维数降序取出前 $\frac{m}{2} \times \frac{n}{2}$ 个分数盒维数对应的图像块 Y'_i , 组成一个有序特征块集合; 并从 Y 的图像块中取出与 Y'_i 位置相同的图像块 Y_i , 组成待检测图像的有序特征块集合; 对这些图像块分别进行一级小波分解, 得到逼近子图 LL'_i, LL_i ; 用密钥 key_2 按照步骤5中的方法生成 $R_1(p), R_2(p)$, 然后利用公式:

$$\hat{Y}_i = \begin{cases} \frac{LL_i - LL'_i}{R_1(p) \times Y}, p = 1, 2, \dots, \frac{m}{4} \times \frac{n}{2} \\ \frac{LL_i - LL'_i}{R_1(p) \times Y}, p = \frac{m}{4} \times \frac{n}{2} + 1, \dots, \frac{m}{2} \times \frac{n}{2} \end{cases} \quad (5)$$

将所有的 \hat{Y}_i 按从左到右、从上到下的顺序组成方阵 \hat{Y} 。

步骤5 将 \hat{Y} 与 K' 进行异或运算, 得到水印图像 \hat{L} , 再用密钥 key_1 对其进行 Arnold 反变换, 从而得到最终的水印图像 L_1 。同样的方法用密钥 key_1, key_3 可得 L_2 , 取 $L = (L_1 + L_2)/2$, 把 L 转化为二值图像, 即得提取的水印 L 。

3 实验结果及分析

为验证文中算法的有效性, 实验中采用 512×512 的 RGB 彩色丽娜图像作为原始载体图像进行实验, 如图 1(a) 所示。二值水印图像, 如图 2(a) 所示, 通过六

次 Arnold 变换以及二维 Logistic 混沌加密得到水印图像, 按上述算法将其嵌入到原始图像, 得到嵌入水印后的图像。



(a) 原始丽娜图

数字
水印



(b) 原始水印

(c) 置乱加密水印



(d) 含水印丽娜图

数字
水印

(e) 提取的水印

图1 水印嵌入效果图

数字
水印

(a) 原始水印



(b) Arnold 置乱水印



(c) 二维 Logistic 混沌加密水印

数字
水印

(d) 密钥正确时提取的水印

图2 水印预处理

3.1 水印预处理效果图

图 2(a) 为原始水印, 经过 Arnold 六次置乱得到置乱水印, 如图 2(b)。密钥是选择控制参数为 $\mu_1 = \mu_2 = \mu = 0.9, v = 0.13$, 初始点为 $(x_0, y_0) = (0.10, 0.20)$, 用具有对称一次耦合项的二维 Logistic 混沌映射序列迭代得到两组矩阵 X, Y , 如图 3 所示, 再经过一系列处理得到置乱矩阵 K' 。

3.2 水印嵌入和提取的视觉效果

图 1(a) 是要嵌入水印的原始丽娜图像, 在水印的嵌入时, 利用像素八邻域算法将水印嵌入到彩色图像的亮度分量中。图 1(d) 是嵌入水印后得到的图像。通过计算, 其峰值信噪比 PSNR 为 40.9263, 在对嵌入水印后图像未做任何修改的情况下检测水印, 水印信息误码率 ErrorRatio 值为 0。

从图 1 可以看出,嵌入水印后图像在视觉上并没有发生明显的降质。

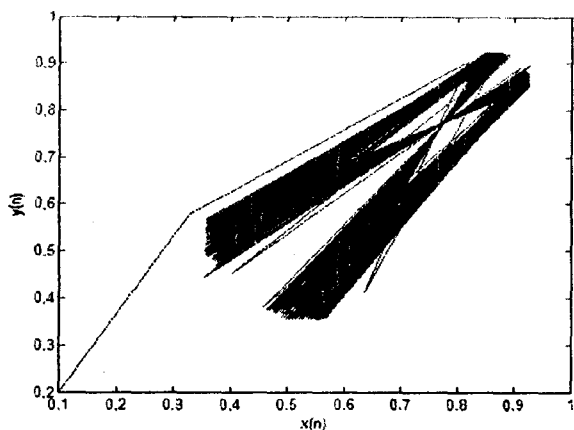


图 3 二维 Logistic 混沌信号状态图

3.3 常见图像处理鲁棒性分析

为验证算法,以峰值信噪比 PSNR/dB 和归一化相似度 NC 为评价标准^[14],分别对嵌入水印的丽娜图像进行不同的攻击,提取出来的水印图像与原水印的峰值信噪比和相似度如表 1 所示。

表 1 抗 JPEG 压缩参数表

JPEG 压缩 的质量因子	指标	二维混沌加 密算法嵌入 彩色丽娜图	未加密算法嵌 入彩色丽娜图
未受攻击	PSNR/dB	42.4508	40.9264
	NC	1	1
100	PSNR/dB	36.7243	36.2334
	NC	1	1
90	PSNR/dB	34.1555	33.8835
	NC	0.9788	0.9743
80	PSNR/dB	32.5323	32.4120
	NC	0.9327	0.9251
70	PSNR/dB	31.7667	31.6426
	NC	0.8955	0.8951
60	PSNR/dB	31.1331	30.9794
	NC	0.8714	0.8671

表 2 抗其他常见图像攻击参数表

攻击 类型	参数	指标	二维混沌加 密算法嵌入 彩色丽娜图	未加密算法嵌 入彩色丽娜图
噪声	椒盐	PSNR/dB	30.9607	30.6051
		NC	0.9852	0.9458
	高斯	PSNR/dB	31.2986	31.2030
		NC	0.8720	0.8714
滤波	中值	PSNR/dB	30.9711	30.8912
	[3 3]	NC	0.8321	0.8312
剪切	25%	PSNR/dB	20.3073	17.2336
		NC	0.9071	0.9070
	50%	PSNR/dB	13.9608	10.9589
		NC	0.8816	0.8772

从表 1、2 及图 4 可以看出,该算法对图像的压缩、加噪、剪切等攻击都具有很好的鲁棒性。

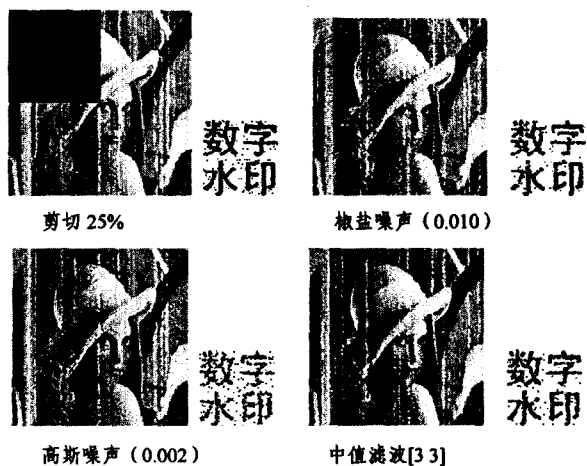


图 4 受攻击的含水印丽娜图及提取的水印

4 结束语

提出了一种新的兼具水印高安全性的彩色图像水印算法,对水印实施 Arnold 变换、二维混沌加密等预处理,增强水印信息的安全性算法。该方法充分利用图像自身的特征,用分数盒维数分析彩色图像亮度分量块的特征,提取特征块和次特征块,将置乱后的水印以不同强度自适应地嵌入到特征块的小波域低频子图中,在保证隐蔽性的前提下,再次将置乱后的水印以不同强度嵌入到次特征块的小波域低频子图中。实验结果表明,该算法不仅具有高安全性,而且对于嵌入水印后的图像具有良好的不可见性,对图像的压缩加噪、剪切攻击等具有较好的鲁棒性。

参考文献:

- [1] Chen G R, Mao Y B. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons & Fractals, 2004, 21(7): 49-61.
- [2] Chiaraluce F, Cicarelli L. A new chaotic algorithm for video encryption[J]. IEEE Trans Consum Electron, 2002, 48(4): 838-844.
- [3] 焦占亚,王蕊. 时空二维混沌的 JPEG2000 数字水印算法研究[J]. 计算机与数字工程, 2008, 36(3): 108-113.
- [4] 刘英,孙丽莎. 基于三维猫映射的图像加密算法[J]. 计算机工程与应用, 2005, 41(36): 127-130.
- [5] Shi C, Bhargara B. Light-Weigh MPEG video encryption algorithm[C]// In: Proceeding of the International conference on Multimedia'98. New Delhi, India: [s. n.], 1998: 55-61.
- [6] 齐东旭,邹建成. 一类新的置乱变换及其在图像信息隐蔽中的应用[J]. 中国科学, 2000, 30(5): 440-447.
- [7] 罗维潮,付永庆. 一种基于小波变换的二维 Logistic 混沌图像加密算法[J]. 黑龙江工程学院学报: 自然科学版, 2007, 6(2): 30-43.

冲机制来保证界面的平滑变换,从整个视觉效果上来讲,车辆的状态演化过程相当明显,车辆的运行行为十分贴近现实。

在进行数值模拟时,每个样本运行 30800 时步,为了消除暂态的影响,只对最后 800 个时步的数值模拟结果作时间平均;由于初始分布是随机的,故取 20 个样本作系统平均,以减小随机性的影响,图 1、图 2 中的每个点是 20 次运行的平均值。

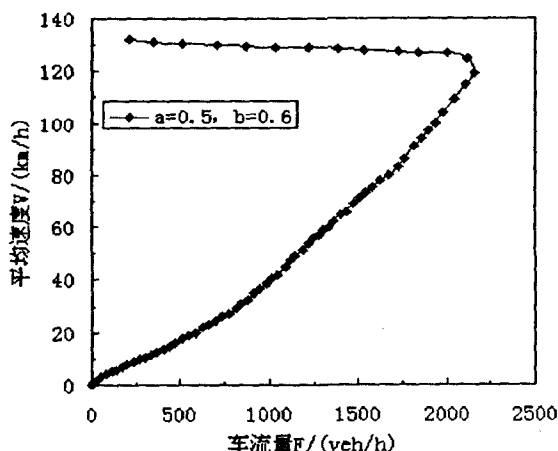


图 1 数值模拟得到的流量-平均速度关系基本图

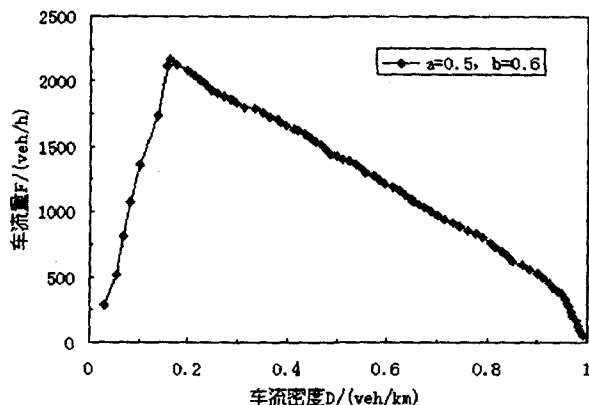


图 2 数值模拟得到的密度-流量关系基本图

从以上两图可以看出,当指数参数 $a = 0.5, b = 0.6$ 时最大车流量为 2203 veh/h,非常接近于实际高速公路的基本通行能力(2200 veh/h)^[7]。在低密度的自

由流阶段,所有车辆都以自己期望的速度值行驶,因此系统的平均速度大致等于最大允许速度;随着车辆密度的增大,系统中的车辆逐渐受到其他车辆的影响,车辆速度缓慢减小,车流量则继续增大;随着车流密度的继续增加,车流状态逐渐由自由流转变成为拥挤流,局部车流段开始出现堵塞区,从而导致车流量的急剧下降,在基本图上的具体表现为曲线从最大流量点快速回归到速度、流量都为零的原点。

3 结束语

agent 技术作为人工智能领域的最新技术,为进行交通问题研究提供了有效的方法。基于 agent 的智能交通仿真研究有助于真正实现从交通个体的角度模拟其行为,并且考虑到与其他交通个体和环境之间的信息交流的特点,能够在仿真系统中实现个体的智能感知、决策和行为反应等特征,这样既能准确地模拟交通实体的微观运行特性,又能满足交通系统复杂性、实时性的需要,从而实现交通系统真正的智能控制。

参考文献:

- [1] 赵建有,赵丽平. 基于多智能体的城市交通流控制原型系统[J]. 交通运输工程学报, 2003, 3(3): 101-105.
- [2] Wolfram S. Theory and Application of Cellular Automata [M]. Singapore: World Scientific, 1986.
- [3] 王宏生. 人工智能及其应用[M]. 北京: 国防工业出版社, 2006.
- [4] Ashri, Ronald, Luck, et al. From SMART To Agent Systems Development[J]. Engineering Applications of Artificial Intelligence, 2005, 18(2): 129-140.
- [5] 孙宪鹏, 张宇, 王成恩, 等. 基于 KQML 语言的合同网协议模型及实现[J]. 信息与控制, 2000, 29(5): 454-460.
- [6] 程晓明, 李文权. 元胞自动机交通流模型的随机规则[J]. 交通运输工程与信息学报, 2007, 5(3): 96-99.
- [7] 中华人民共和国交通部. JTG B01-2003 公路工程技术标准[S]. 北京: 人民交通出版社, 2004.

(上接第 144 页)

- [8] 丁文霞, 卢焕章, 王浩, 等. 一种基于混沌的彩色图像空域半脆弱水印算法[J]. 国防科技大学学报, 2008, 30(4): 59-63.
- [9] 王丽娜, 郭迟, 李鹏. 信息隐藏技术实验教程[M]. 武汉: 武汉大学出版社, 2004.
- [10] 姜炳强, 江铭炎, 赵立军. 一种新的基于小波变换与混沌加密的彩色数字水印算法[J]. 山东大学学报, 2004, 34(3): 68-71.
- [11] 陈颢, 陈凌. 分形几何学[M]. 第 2 版. 北京: 地震出版

社, 2005: 54-71.

- [12] Feng J. Fractional fractal geometry for image processing[D]. USA: Northwestern University, 2000.
- [13] Ni Rongrong, Ruan Qiuqi, Cheng H D. Secure semi-blind watermarking based on iteration mapping and image features[J]. Pattern Recognition, 2005, 38: 357-368.
- [14] 余成波. 数字图像处理及 MATLAB 实现[M]. 重庆: 重庆大学出版社, 2003.